BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 08. 2023 - 15. 08. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01794/2022/SK-CERT-1285

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Intel produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností. Oprava predmetných zraniteľnosti okrem aktualizácie aplikačného softvéru vyžaduje aj aktualizáciu firmvéru.

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte AI Hackathon, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.08.2023

CVE

CVE-2022-27635, CVE-2022-27879, CVE-2022-29470, CVE-2022-29871, CVE-2022-29887, CVE-2022-34657, CVE-2022-36351, CVE-2022-36372, CVE-2022-36392, CVE-2022-37336, CVE-2022-37343, CVE-2022-38076, CVE-2022-38083, CVE-2022-38102, CVE-2022-38973, CVE-2022-40964, CVE-2022-40982, CVE-2022-41804, CVE-2022-41984, CVE-2022-43456, CVE-2022-43505, CVE-2022-44611, CVE-2022-44612, CVE-2022-45112, CVE-2022-46329, CVE-2023-22276, CVE-2023-22330, CVE-2023-22338, CVE-2023-22356, CVE-2023-22444, CVE-2023-22449, CVE-2023-22840, CVE-2023-22841, CVE-2023-23577, CVE-2023-24016, CVE-2023-25182, CVE-2023-25757, CVE-2023-25773, CVE-2023-25775, CVE-2023-25944, CVE-2023-26587, CVE-2023-27391, CVE-2023-27392, CVE-2023-27505, CVE-2023-27506, CVE-2023-27509, CVE-2023-27515, CVE-2023-27887, CVE-2023-28380, CVE-2023-28385, CVE-2023-28405, CVE-2023-28711, CVE-2023-28714, CVE-2023-28736, CVE-2023-28823, CVE-2023-28938, CVE-2023-29151, CVE-2023-29243, CVE-2023-29494, CVE-2023-29500, CVE-2023-30760, CVE-2023-31246, CVE-2023-32285, CVE-2023-32543, CVE-2023-32547, CVE-2023-32609, CVE-2023-32617, CVE-2023-32656, CVE-2023-32663, CVE-2023-33867, CVE-2023-33877, CVE-2023-34086, CVE-2023-34349, CVE-2023-34355, CVE-2023-34427, CVE-2023-34438

Zasiahnuté systémy

Intel® PCSD BIOS vo verzii staršej ako 02.01.0013
Intel® PROSet/Wireless WiFi software vo verzii staršej ako 22.200
Intel® CSME software installer vo verzii staršej ako 2306.4.10.0
Intel® CSME, Intel® AMT a Intel® Standard Manageability vo verzii staršej ako 3.1.94, 4.0.48, 11.12.94, 11.22.94, 11.8.94, 12.0.93, 13.0.65, 13.30.35, 13.50.25, 14.1.70, 14.5.50, 15.0.45, a 16.1.27
Intel® Ethernet Controller RDMA driver pre linux vo verzii staršej ako 1.9.30
Intel® RST software vo verzii staršej ako 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1010.3 a 19.5.2.1049.5
Intel® Quartus® Prime Pro edition software pre Linux vo verzii staršej ako 22.4
Intel® Quartus® Prime Standard edition software pre Linux vo verzii staršej ako 22.1STD
Intel® Arc™ graphics cards A770 a A750 predané medzi októbrom 2022 a decembrom 2022
Intel Atom® processor C3000 series
Intel® Xeon® D Processor
Intel Atom® processor P5000 series
Intel® Xeon® E Processor Family

11th Gen Intel® Core™ Processor Family
10th Gen Intel® Core™ Processor Family
Intel® Xeon® W processor 1300 series
9th Gen Intel® Core™ Processor Family
8th Gen Intel® Core™ Processor Family
8th Generation Intel® Core™ Processors
Intel® Celeron® J6413, N6211
Intel® Pentium® J6425, N6415
Intel® Atom® x6211E, x6413E, x6425E
x6212RE, x6414RE, x6425RE, x6427FE, x6200FE
Intel® Pentium® Processor J Series
Intel® Pentium® Processor N Series
Intel® Celeron® Processor J Series
Intel® Celeron® Processor N Series
Intel® Atom® Processor A Series
Intel® Atom® Processor E3900 Series
Intel® Pentium® Processor Silver Series
Intel® Xeon® Processor E7 v4 Family
Intel® Xeon® Processor E5 v4 Family
Intel® Core™ X-series Processors
Intel® Xeon® Processor E7 v3 Family
Intel® Xeon® Processor E5 v3 Family
Intel® Xeon® Processor D Family
Intel® Xeon® D-1633N Processor
3rd Generation Intel® Xeon® Scalable Processor Family
Intel® Denverton Atom® Processor C3XXX
Intel® Xeon® Processor E3 v6 Family
10th Generation Intel® Core™ Processor Family
Intel® Core™ Processors with Intel® Hybrid Technology
Intel® Xeon® Processor W Family
2nd Generation Intel® Xeon® Scalable Processors
Intel® Xeon® Scalable Processors
8th Generation Intel® Core™ Processor Family
7th Generation Intel® Core™ Processor Family
Intel® Pentium® Gold Processor Series
Intel® Celeron® Processor G Series
9th Generation Intel® Core™ Processor Family
Intel® oneVPL GPU Runtime software vo verzii staršej ako 22.6.5
Intel® Unite® Client software pre Mac vo verzii staršej ako 4.2.11
Intel® Unite® Hub software installer pre Windows vo verzii staršej ako Release 4.2.34962
ITE Tech consumer infrared drivers vo verzii staršej ako 5.5.2.1 pre Intel® NUC
System Firmware Update Utility (SysFwUpdt) pre Intel® Server Boards and Intel® Server Systems Based on Intel® 621A Chipset vo verzii staršej ako 16.0.7
Intel® Ethernet Network Controllers and Adapters E810 (Columbiaville) Series vo verzii staršej ako 1.7.2.4
3rd Gen Intel® Xeon® Scalable Processor family
Intel® Xeon® D Processors
4th Generation Intel® Xeon® Scalable Processors
Intel® Optimization pre TensorFlow software vo verzii staršej ako 2.12
Intel® Distribution of OpenVINO™ Toolkit vo verzii staršej ako 2022.3.0

Intel® VCUST Tool software stiahnutý pred Feb 3, 2023
Intel® VROC software vo verzii staršej ako 8.0.0.4035
Intel® Advanced Link Analyzer Standard Edition software installer vo verzii staršej ako 22.1.1
Intel® ISPC software installer pre Windows vo verzii staršej ako 1.19.0
Intel Agilex® software pre linux vo verzii staršej ako 22.4
Intel® Easy Streaming Wizard software vo všetkých verziách
Intel® Support android application vo verzii staršej ako v23.02.07
Intel® NUC Pro Software Suite pre Windows vo verzii staršej ako 2.0.0.9
Intel® PROSet/Wireless WiFi 6 AX200 software vo verzii staršej ako 22.220 HF
Intel® DTT Software vo verzii staršej ako 8.7.10801.25109
Intel® AI Hackathon software vo verzii staršej ako 2.0.0
Intel® DSA software vo verzii staršej ako 23.1.9
Hyperscan Library maintained by Intel® vo verzii staršej ako 5.4.1
Intel® oneAPI Toolkits vo verzii staršej ako 2023.1.0
Intel® NUC Boards
Intel® NUC Performance Kit, Intel® NUC Performance Mini PC
Intel® NUC 11 Performance Kit, Intel NUC 11 Performance Mini PC
Intel® Manageability Commander software vo verzii staršej ako 2.3
Intel® Unison™ software vo verzii staršej ako 10.12
Intel® Server Board M10JNP2SB Integrated BMC Video Drivers pre Microsoft Windows vo verzii staršej ako 3.0
Intel® Server Board M10JNP2SB Integrated BMC Video Drivers pre Linux vo verzii staršej ako 1.13.4
Intel® ITS software vo verzii staršej ako 3.1
MAVinci Desktop software pre Intel® Falcon 8+ vo všetkých verziách
Intel Unite® android application vo verzii staršej ako 4.2.3504
Intel® NUC 7 Enthusiast
Intel® NUC Kit
Intel® NUC Board
Intel® NUC 13 Extreme Compute Element
Intel® NUC 13 Extreme Kit
Intel® NUC Performance Kit and Mini PC
Intel® NUC 8 Compute Element
Intel® NUC Pro Kit, Intel NUC Pro Board
Intel® NUC 11 Compute Element
Intel® NUC 12 Compute Element
Intel® NUC Extreme, Intel® NUC 12 Extreme Compute Element
Intel® NUC Laptop Kit
Intel® NUC Pro Board, Intel® NUC Pro Kit
Intel® NUC Laptop Kits
Intel® NUC Enthusiast
Intel® NUC Essential
Intel® NUC Extreme Compute Element
Intel® NUC
Intel® NUC Pro Compute Element
Intel® NUC Rugged Kit
Intel® NUC Business, Intel® NUC Enthusiast, Intel® NUC Kit
Intel® NUC Pro Kit, Intel® NUC Pro Board, Intel® NUC Pro Mini PC
Intel® NUC Mini PC, Intel® NUC Kit, Intel® NUC Enthusiast, Intel® NUC Board
Intel® Compute Element
Intel® RealSense™ ID software pre Intel® RealSense™ 450 FA vo verzii staršej ako 0.25

Intel® PSR SDK vo verzii staršej ako 1.0.0.20.
The Intel® SDP Tool software vo verzii staršej ako 1.4 build 5
Intel® SSD Tools software vo verzii staršej ako mdadm-4.2-rc2
Intel® RealSense™ SDK vo verzii staršej ako 2.53.1

Následky
Eskalácia privilégií Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru. Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00742.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00766.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00783.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00794.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00795.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00800.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00812.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00813.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00818.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00826.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00828.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00829.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00830.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00835.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00837.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00840.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00842.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00842.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00844.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00846.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00848.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00849.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00850.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00859.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00862.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00868.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00872.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00875.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00877.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00878.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00879.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00890.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00893.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00897.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00899.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00938.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00934.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00932.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00917.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00912.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00907.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00905.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00690.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00946.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Elecom & Logitec sieťové zariadenia - viacero bezpečnostných zraniteľností

Popis

Spoločnosti Elecom a Logitec vydali bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.08.2023

CVE

CVE-2023-32626, CVE-2023-35991, CVE-2023-38132, CVE-2023-38576, CVE-2023-39445, CVE-2023-39454, CVE-2023-39455, CVE-2023-39944, CVE-2023-40069, CVE-2023-40072

Zasiahnuté systémy

Sieťové zariadenia Elecom a Logitec
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

http://jvn.jp/en/vu/JVNVU91630351/index.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produktoch Acrobat, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.08.2023

CVE

CVE-2023-29299, CVE-2023-29303, CVE-2023-29320, CVE-2023-38210, CVE-2023-38211, CVE-2023-38212, CVE-2023-38213, CVE-2023-38222, CVE-2023-38223, CVE-2023-38224, CVE-2023-38225, CVE-2023-38226, CVE-2023-38227, CVE-2023-38228, CVE-2023-38229, CVE-2023-38230, CVE-2023-38231, CVE-2023-38232, CVE-2023-38233, CVE-2023-38234, CVE-2023-38235, CVE-2023-38236, CVE-2023-38237, CVE-2023-38238, CVE-2023-38239, CVE-2023-38240, CVE-2023-38241, CVE-2023-38242, CVE-2023-38243, CVE-2023-38244, CVE-2023-38245, CVE-2023-38246, CVE-2023-38247, CVE-2023-38248

Zasiahnuté systémy

Acrobat DC vo verzii staršej ako 23.003.20269
Acrobat Reader DC vo verzii staršej ako 23.003.20269
Acrobat 2020 pre Mac vo verzii staršej ako 20.005.30516.10516
Acrobat 2020 pre Win vo verzii staršej ako 20.005.30514.10514
Acrobat Reader 2020 pre Mac vo verzii staršej ako 20.005.30516.10516
Acrobat Reader 2020 pre Win vo verzii staršej ako 20.005.30514.10514
Acrobat DC Continuous vo verzii staršej ako 23.003.20269
Adobe XMP-Toolkit-SDK vo verzii staršej ako 2023.07
Adobe Dimension vo verzii staršej ako 3.4.10

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje
https://helpx.adobe.com/security/products/acrobat/apsb23-30.html
https://helpx.adobe.com/security/products/xmpcore/apsb23-45.html
https://helpx.adobe.com/security/products/dimension/apsb23-44.html
https://www.securityweek.com/patch-tuesday-adobe-patches-30-acrobat-reader-vulns/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

AMD produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť AMD vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností. Oprava predmetných zraniteľnosti okrem aktualizácie aplikačného softvéru vyžaduje aj aktualizáciu firmvéru.

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte AMD RyzenTM Master, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.08.2023

CVE

CVE-2022-27677, CVE-2022-3602, CVE-2022-3786, CVE-2023-20555, CVE-2023-20556, CVE-2023-20560, CVE-2023-20561, CVE-2023-20562, CVE-2023-20564, CVE-2023-20569, CVE-2023-20586, CVE-2023-20588, CVE-2023-20589

Zasiahnuté systémy

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7005.html
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7003.html
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7004.html
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-4003.html
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7001.html
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7007.html
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-6007.html
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-4005.html
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1052.html
https://explore.alas.aws.amazon.com/CVE-2023-20564.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.0
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Tlačiarne Lexmark - bezpečnostná zraniteľnosť

Popis

Spoločnosť Lexmark vydala bezpečnostné aktualizácie na svoje portfólio tlačiarní, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. V prípade, že tlačiareň nemá nastavený administrátorský účet, je zraniteľnosť zneužiteľná aj bez potreby autentifikácie.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

13.03.2023

CVE

CVE-2023-26067

Zasiahnuté systémy

Lexmark tlačiarne
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://publications.lexmark.com/publications/security-alerts/CVE-2023-26067.pdf
https://github.com/horizon3ai/CVE-2023-26067

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Schneider Electric IGSS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt Interactive Graphical SCADA System, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.08.2023

CVE

CVE-2023-3001

Zasiahnuté systémy

IGSS Dashboard vo verzii staršej ako 16.0.0.23131

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-220-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell DSITV - zabudovaný účet s predvoleným heslom

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Storage Integration Tools for VMware.
Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.08.2023

CVE

CVE-2023-39250

Zasiahnuté systémy

Dell Storage Integration Tools for VMware (DSITV) vo verzii staršej ako 06.01.00.016 (vrátane)

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Výrobca odporúča zmeniť predvolené prihlasovacie heslo, detailné inštrukcie môžete nájsť na webovej adrese:
https://dl.dell.com/content/manual53920915-dell-storage-integration-tools-for-vmware-version-6-1-administrator-s-guide.pdf

Zdroje

https://www.dell.com/support/kbdoc/sk-sk/000216615/dsa-2023-282-security-update-for-dell-storage-integration-tools-for-vmware-dsitv-vulnerabilities
https://www.bleepingcomputer.com/news/security/dell-compellent-hardcoded-key-exposes-vmware-vcenter-admin-creds/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Hitachi Energy RTU500 series - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hitachi Energy vydala bezpečnostnú aktualizáciu na svoje moduly série RTU500, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka spôsobiť zneprístupnenie služby. Pre zneužitie zraniteľnosti musí byť funkcia HCI 60870-5-104 nakonfigurovaná s podporou IEC 62351-3.

Dátum prvého zverejnenia varovania

08.08.2023

CVE

CVE-2022-2502, CVE-2022-4608

Zasiahnuté systémy

CMU firmvér vo verzii staršej ako 13.3.3 alebo 13.4.1.

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-220-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PostgreSQL - bezpečnostná zraniteľnosť

Popis

Vývojári databázového systému PostgreSQL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.08.2023

CVE

CVE-2023-39417

Zasiahnuté systémy

PostgreSQL 15 vo verzii staršej ako 15.4
PostgreSQL 14 vo verzii staršej ako 14.9
PostgreSQL 13 vo verzii staršej ako 13.12
PostgreSQL 12 vo verzii staršej ako 12.16
PostgreSQL 11 vo verzii staršej ako 11.21

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Databázové systémy odporúčame prevádzkovať v kontajnerizovanom prostredí.

Zdroje

https://www.postgresql.org/support/security/CVE-2023-39417/
https://www.securitynewspaper.com/2023/08/14/hacking-postgresql-applications-with-a-sql-injection-vulnerability/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

FortiOS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Fortinet vydala bezpečnostnú aktualizáciu na svoj produkt FortiOS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.08.2023

CVE

CVE-2023-29182

Zasiahnuté systémy

FortiOS vo verzii staršej ako 7.4.0
FortiOS vo verzii staršej ako 7.2.0
FortiOS vo verzii staršej ako 7.0.4

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.fortiguard.com/psirt/FG-IR-23-149